World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:11, No:02, 2017

A Characterization of Skew Cyclic Code with Complementary Dual

Authors : Eusebio Jr. Lina, Ederlina Nocon

Abstract : Cyclic codes are a fundamental subclass of linear codes that enjoy a very interesting algebraic structure. The class of skew cyclic codes (or θ-cyclic codes) is a generalization of the notion of cyclic codes. This a very large class of linear codes which can be used to systematically search for codes with good properties. A linear code with complementary dual (LCD code) is a linear code C satisfying C ∩ C^⊥ = {0}. This subclass of linear codes provides an optimum linear coding solution for a two-user binary adder channel and plays an important role in countermeasures to passive and active side-channel analyses on embedded cryptosystems. This paper aims to identify LCD codes from the class of skew cyclic codes. Let F_q be a finite field of order q, and θ be an automorphism of F_q. Some conditions for a skew cyclic code to be LCD were given. To this end, the properties of a noncommutative skew polynomial ring F_q[x, θ] of automorphism type were revisited, and the algebraic structure of skew cyclic code using its skew polynomial representation was examined. Using the result that skew cyclic codes are left ideals of the ring F_q[x, θ]/⟨x^n-1⟩, a characterization of a skew cyclic LCD code of length n was derived. A necessary condition for a skew cyclic code to be LCD was also given.

Keywords : LCD cyclic codes, skew cyclic LCD codes, skew cyclic complementary dual codes, theta-cyclic codes with complementary duals
Conference Title : ICCTC 2017 : International Conference on Coding Theory and Cryptography
Conference Location : Kuala Lumpur, Malaysia
Conference Dates : February 12-13, 2017